UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

EVERETT TURNER, **on behalf of himself and all others similarly situated,** **Plaintiff,** **v.** **FLAGSTAR BANK, FSB,** **Defendant.**	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Everett Turner ("Plaintiff"), by and through him attorneys, upon personal knowledge as to himself and his own acts and experiences, and upon information and belief as to all other matters, alleges as follows:

NATURE OF THE ACTION

1. Plaintiff brings this Class Action Complaint ("Complaint") against Defendant Flagstar Bank, FSB ("Flagstar" or "Defendant"), individually and on behalf of himself and all others similarly situated ("Class" or "Class Members") based on Defendant's failure to properly safeguard personally identifiable information ("PII") that it stored on and/or shared using its vendor's file sharing platform, including without limitation, Social Security numbers, account numbers, name, address, dates of birth, and/or financial institution name.

2. According to its website, Defendant "has assets of $23.2 billion, [and] is the sixth largest bank mortgage originator nationally."[1] Defendant "operate[s] 150 branches in Michigan,

[1] https://www.flagstar.com/about-flagstar.html (last visited 7/1/2022).

Indiana, California, Wisconsin, and Ohio and provide a full complement of products and services for consumers and businesses."[2]

3. Defendant's "mortgage division operates nationally through 82 retail locations and a wholesale network of approximately 2,700 third-party mortgage originators."[3] Defendant is "also a leading servicer and subservicer of mortgage loans—handling recordkeeping for $300 billion in home loans."[4]

4. On or before June 2, 2022, Defendant learned that an unauthorized actor breached Defendant's network in December 2021.[5]

5. On or before June 2, 2022, Defendant concluded its forensic investigation and document review, and began notifying individuals who were impacted.[6]

6. Through its investigation, Defendant learned that the unauthorized actor removed one or more documents that contained the PII of Plaintiff and Class Members, including, but not limited to, Social Security numbers, account numbers, name, address, dates of birth, and/or financial institution name.[7]

7. Flagstar did not adequately safeguard Plaintiff's data, and now she and apparently many other individuals are the victims of a significant data breach that will negatively affect them for the rest of their lives.

8. Flagstar is responsible for allowing this data breach through its failure to implement and maintain reasonable safeguards and its failure to comply with industry-standard data security practices.

---

[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] https://www.flagstar.com/customer-support/customer-data-information-center.html (last accessed July 1, 2022).
[6] *Id.*
[7] *See* Notice Letter, Exhibit A.

9. Flagstar had numerous statutory, regulatory, contractual, and common law obligations, including those based on its affirmative representations to Plaintiff and Class Members, to keep their PII confidential, safe, secure, and protected from unauthorized disclosure or access.

10. Plaintiff and those similarly situated rely upon Flagstar to maintain the security and privacy of the PII entrusted to it; when providing their PII, they reasonably expected and understood that Flagstar would comply with its obligations to keep the information secure and safe from unauthorized access.

11. In this era of regular and consistent data security attacks and data breaches, in particular in the financial services industry, Flagstar's data security breach is particularly egregious.

12. As a result of Flagstar's failures, Plaintiff and the Class Members are at a significant risk of identity theft, financial fraud, and/or other identity-theft or fraud, imminently and for years to come.

13. Just as their PII was stolen because of its inherent value in the black market, now the inherent value of Plaintiff's and the Class Members' PII in the legitimate market is significantly and materially decreased.

14. On information and belief, as a result of this massive data breach, more than 1 million individuals have suffered exposure of PII entrusted to Flagstar.

15. In addition, based on Defendant's actions, Plaintiff and the proposed Class have received services that were and are inferior to those for which they have contracted, and have not been provided the protection and security Flagstar promised when Plaintiff and the proposed Class entrusted Flagstar with their PII.

16. Plaintiff and members of the proposed Class have suffered actual and imminent injuries as a direct result of the data breach. The injuries suffered by Plaintiff and the proposed Class as a direct result of the data breach include: (a) theft of their personal data; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the consequences of the data breach and the stress, nuisance and annoyance of dealing with all issues resulting from the data breach; (d) the imminent injury arising from potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (e) damages to and diminution in value of their personal data entrusted to Flagstar and with the mutual understanding that Flagstar would safeguard Plaintiff's and Class Members' personal data against theft and not allow access and misuse of their personal data by others; (f) the diminution in value of the PII entrusted to Flagstar; and (g) the continued risk to their personal data, which remains in the possession of Flagstar and which is subject to further breaches so long as Flagstar fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' personal data in its possession.

17. Plaintiff seeks to remedy these harms, and prevent their future occurrence, on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the data breach.

18. Accordingly, Plaintiff, on behalf of himself and other members of the Class, asserts claims for negligence, bailment, breach of implied contract, unjust enrichment, and violation of the Indiana Deceptive Consumer Sales Act. Plaintiff seeks injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

Plaintiff Everett Turner

19. Plaintiff Everett Turner is a resident of Platte City, Missouri and a customer of Flagstar. On or about June 16, 2022, Plaintiff received a notice from Defendant regarding its December 3-4, 2021 Data Breach. *See* attached as Exhibit A.

Defendant Flagstar

20. Defendant Flagstar Bank, FSB is a Michigan-based federally chartered stock savings bank, headquartered at 5151 Corporate Drive, Troy, Michigan.

JURISDICTION & VENUE

21. This Court has original jurisdiction under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a Class action involving more than 100 putative Class Members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Many members of the putative class are citizens of different states thereby satisfying CAFA's minimal diversity requirement.

22. This Court has general personal jurisdiction over Defendant because Defendant is headquartered in this District and Defendant conducts substantial business in Michigan and this District through its headquarters, officers, parents, and affiliates.

23. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant conducts substantial business in this District.

FACTUAL ALLEGATIONS

24. On or about December 3, 2021, and December 4, 2021, Flagstar experienced a cyber incident that involved unauthorized access to its network.

25. On June 2, 2022, after a forensic investigation and document review, Flagstar discovered the breach.

26. Flagstar sent letters to its customers notifying them of the breach on or about June 16, 2022.

27. As with all financial banking institutions, use of Flagstar's financial services requires disclosure of PII to Flagstar by its customers, including Plaintiff and Class Members.

28. Flagstar is fully aware of how sensitive the PII it stores and maintains is. It is also aware of how much PII it collects, uses, and maintains from each Plaintiff or Class Member.

29. By requiring the production of, collecting, obtaining, using, and deriving benefits from Plaintiff's and the Class Members' PII, Flagstar assumed certain legal and equitable duties and knew or should have known that it was responsible for the diligent protection of the PII it collected and stored.

Flagstar Knew it Was and Continues to be a Prime Target for Cyberattacks

30. Flagstar knew it was an ideal target for hackers and those with nefarious purposes related to customer and employee data. It processed and saved multiple types and many levels of PII.

31. Yet, Flagstar did not follow generally accepted industry standards to protect the sensitive PII entrusted to it.

32. Flagstar processed all of the personal and financial information that it demands from its customers as a financial services and banking institution, such as full names, Social Security numbers, residential addresses, phone numbers, tax ID numbers, dates of birth, and/or financial account information.

33. The seriousness with which Defendant should have taken its data security is shown

by the number of data breaches perpetrated in the financial industry over the last few years, including prior data breaches involving Flagstar and one of its vendors, Accellion.

34. Despite knowledge of the prevalence of financial data breaches, Defendant failed to prioritize its customers' data security by implementing reasonable data security measures to detect and prevent unauthorized access to the sensitive data points of its millions of customers.

35. As a highly successful multibillion dollar company, Flagstar had the resources to invest in the necessary data security and protection measures. Yet, it did not—instead, consciously disregarding the known risks.

36. Defendant failed to undertake adequate analyses and testing of its own systems, adequate personnel training, and other data security measures to avoid the failures it notified its customers of in mid-June 2022, but which occurred over 6 months before in December of 2021.

37. Despite its awareness, Defendant did not take the necessary and required minimal steps to secure Plaintiff's and the Class Members' PII. As a result, hackers breached and stole important PII from more than one million of Flagstar's customers.

Defendant Owed a Duty to Adequately Safeguard Consumers' PII

38. Defendant is aware of the importance of security in maintaining personal information (particularly sensitive personal and financial information), and the value its users place on keeping their PII secure.

39. Defendant owes a duty to Plaintiff and the Class Members to maintain adequate security and to protect the confidentiality of their PII.

40. Defendant owes a further duty to its customers and employees to immediately and accurately notify them of a breach of its systems to protect them from identity theft and other misuse of their personal data and to take adequate measures to prevent further breaches.

The Sort of PII at Issue Here is Particularly Valuable to Hackers

41. Businesses that store sensitive PII are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

42. The unauthorized disclosure of Social Security numbers can be particularly damaging, because Social Security numbers cannot easily be replaced. In order to obtain a new Social Security number a person must prove, among other things, that she or she continues to be disadvantaged by the misuse. Thus, no new Social Security number can be obtained until the damage has been done.

43. Furthermore, as the Social Security Administration ("SSA") warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[8]

44. Here, the unauthorized access by the hackers left the cyber criminals with the tools

[8] SSA, Identity Theft and Your Social Security Number, SSA Publication No. 05-10064 (Dec. 2013), *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited 7/1/2022).

to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. The personal data of Plaintiff and Class Members stolen in the Flagstar security breach constitutes a dream for hackers and a nightmare for Plaintiff and the Class. Plaintiff's and Class Members' stolen personal data represents essentially one-stop shopping for identity thieves.

45. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve, and the FTC has created a website dedicated to instructing consumers what steps they can take to protect their personal information.[9] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[10]

46. More recently the FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

47. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

48. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks;

[9] *See Identity Theft: How to protect your personal information from identity theft*, available at: https://consumer.ftc.gov/identity-theft-and-online-security/identity-theft (last accessed 7/1/2022).
[10] *Id. See also,* https://consumer.ftc.gov/articles/what-know-about-identity-theft#what_is (last accessed 7/1/2022).

understand their network's vulnerabilities; and implement policies to correct any security problems.[11]The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[12]

49. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

50. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

51. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting

[11] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed June 29, 2022).
[12] *Id.*

from data breaches cannot necessarily rule out all future harm.[13]

52. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII on a number of Internet websites. Plaintiff's and Class Members' personal data that was stolen has a high value on both legitimate and black markets.

53. Identity theft is not new or unique, and neither is the need to protect the personal information entrusted in a business's care. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[14]

54. Individuals rightfully place a high value not only on their PII, but also on the privacy of that data. Researchers have already begun to shed light on how much individuals value their data privacy – and the amount is considerable.

55. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[15] This study was done in 2002, about twenty years ago. The sea-change in how pervasive

---

[13] *See* http://www.gao.gov/new.items/d07737.pdf at 29 (last accessed 7/1/2022).
[14] FEDERAL TRADE COMMISSION, *The Information Marketplace: Merging and Exchanging Consumer Data*, *transcript available* at http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data (last accessed 7/1/2022).
[15] Hann, Hui, *et al*, The Value of Online Information Privacy: Evidence from the USA and Singapore, at 17. Oct. 2002, available at https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last accessed 7/1/2022).

the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII to bad actors—would be exponentially higher today.

56. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

57. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns.[16] Former and current Flagstar employees and customers whose Social Security numbers have been compromised will and already have spent time contacting various agencies, such as the Internal Revenue Service and the Social Security Administration. They also now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

58. Again, because the information Defendant allowed to be compromised and taken is of such a durable and near-permanent quality, the harms to Plaintiff and the Class will continue to grow, and Plaintiff and the Class will continue to be at substantial risk for further imminent and future harm.

Flagstar's Post-Breach Activity was Inadequate

59. Personal and financial information can be sold on the black-market almost immediately. As then Illinois Attorney General Lisa Madigan aptly put it, "the second somebody

[16] When fraudulent tax returns are filed, the requirements for a legitimate taxpayer to file their tax returns with the IRS increase, including the necessity to obtain and utilize unique PIN numbers just to be able to file a tax return.

gets your credit or debit card information, it can be a matter of hours or days until it's sold on the black market and someone's starting to make unauthorized transactions."[17] Thus, the compromised information could be used weeks before the receipt of any notification from Flagstar and Flagstar's proposed solutions to the potential fraud are, therefore, woefully deficient.

60. Immediate notice of a security breach is essential to protect people such as Plaintiff and the Class Members. Defendant failed to provide such immediate notice, in fact taking roughly six months to disclose to Plaintiff and Class Members that there had been a breach, thus further exacerbating the damages sustained by Plaintiff and the Class resulting from the breach. Upon information and belief, other Class Members still have not received notice their PII was exposed.

61. Such failure to protect Plaintiff's and the Class Members' PII, and timely notify them of the breach, has significant ramifications. The information stolen allows criminals to commit theft, identity theft, and other types of fraud. Moreover, because many of the data points stolen are persistent—for example, Social Security number, name, and address—as opposed to transitory—criminals who purchase the PII belonging to Plaintiff and the Class Members do not need to use the information to commit fraud immediately. The PII can be used or sold for use years later.

62. Every year, victims of identity theft lose billions of dollars. And reimbursement is only the beginning, as these victims usually spend hours and hours attempting to repair the impact to their credit, at a minimum.

63. Plaintiff and the Class Members are at constant risk of imminent and future fraud, misuse of their PII, and identity theft for many years in the future as a result of the Defendant's

[17] Phil Rosenthal, *Just assume your credit and debit card data were hacked*, http://www.chicagotribune.com/business/columnists/ct-data-breach-credit-scam-rosenthal-1001-biz-20140930-column.html#page=1 (last accessed 7/1/2022).

actions and the data breach. They have suffered real and tangible loss, including but not limited to the loss in the inherent value of their PII, the loss of their time as they have had to spend additional time monitoring accounts and activity, and additional economic loss to mitigate the costs of injuries realized as a result of the breach.

Plaintiff Everett Turner's Experience

64. Plaintiff Everett Turner is a resident of Platte City, Missouri, and at all times relevant to this complaint, was a customer of Flagstar.

65. Plaintiff entrusted Flagstar with his PII, including but not limited to his full name, address, date of birth, Social Security number, income information, and other private financial information. Plaintiff had a reasonable expectation and understanding that Flagstar would, at a minimum, take industry-standard precautions to protect, maintain, and safeguard his private information from unauthorized users or disclosure.

66. On or after June 17, 2022, Plaintiff received a notice from Defendant regarding its December 3-4, 2021 Data Breach. See attached as Exhibit A.

67. Mr. Turner's wife also received a Notice Letter from the Defendant on approximately the same date.

68. In the June 17, 2022 Notice Letter Plaintiff received, Defendant states that "files containing your personal information were accessed and/or acquired from [its] network between December 3, 2021 and December 4, 2021." Exh. A.

69. Defendant disclosed to Plaintiff that "[o]n June 2, 2022, we determined that one or more of the impacted files contained your Social Security number, account/loan number, name, address, date of birth, and financial institution name." Exh. A.

70. Plaintiff is alarmed by the amount of his Private Information that was stolen or

accessed, and even more by the fact that his Social Security number was identified as among the breached data on Defendant's computer system. Yet given the language of the Notice Letter he received, he is still unsure exactly the details of his private information that was accessed and whether it was actually removed from Defendant's network.

71. Plaintiff entrusted Defendant to timely notify him of any data security incidents related to him, but instead, after its data breach, Defendant delayed its notification for over 6 months. During those 6 months, cybercriminals had an unrestricted ability to abuse his private information, including his Social Security number.

72. As a result of learning of the Data Breach, Plaintiff has spent time dealing with the consequences of the Data Breach which includes time spent monitoring news reports to verify the legitimacy of the reports of the Breach and spending time daily checking his financial accounts.

73. Since the data breach, Plaintiff received notice that his private information including his Social Security number has appeared on the Dark Web. In addition, he has been receiving offers for new loans, which he thinks may be related to Defendant's data breach.

74. Plaintiff is aware that cybercriminals often sell Private Information, and that his could be abused months or even years after a data breach. Since learning about the breach, Plaintiff has suffered and continues to suffer anxiety related to the breach of his sensitive personal and financial data. He is uncertain exactly how long he will need to monitor his accounts.

75. Plaintiff knows that he must expend significant time, now and in the future, to reduce his risks as a victim of Defendant's data breach.

76. Had Plaintiff been aware that Defendant's computer systems were not secure, he would not have entrusted Defendant with his Private Information.

Plaintiff and Class Members' Damages

77. To date, Defendant has done absolutely nothing to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach.

78. Moreover, Defendant has offered only a paltry two years of identity theft monitoring and identity theft protection through Kroll. This two-year limitation is inadequate when victims are likely to face many years of identity theft.

79. Defendant's credit monitoring offer and list of "precautionary measures" it offers to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on the Defendant, to monitor and report suspicious activities to law enforcement. In other words, Defendant expects Plaintiff and Class to protect themselves from its tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.

80. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff' and Class Members' PII.

81. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

82. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

83. Plaintiff and Class Members also suffered a loss of value of their Private

Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

84. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Part of the interest and service payments Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer property and Plaintiff' and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for. Specifically, they overpaid for services that were intended to be accompanied by adequate data security but were not.

85. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

86. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

87. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach.

88. In addition, many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach, including:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

89. Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

CLASS ACTION ALLEGATIONS

90. Plaintiff brings all claims as Class claims under Federal Rule of Civil Procedure 23. The requirements of Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3) are met with respect to the Class defined below.

91. Under Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action as a national Class action for himself and all members of the following Class of similarly situated persons:

The Nationwide Class

All individuals whose personally identifiable information was entrusted to Flagstar and was compromised in the December 2021 data breach.

The Missouri Subclass

All Missouri residents whose personally identifiable information was entrusted to Flagstar and was compromised in the December 2021 data breach.

92. Excluded from the Class and Subclass are Defendant; any entity in which

Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

93. Plaintiff reserves the right to modify and/or amend the Class and Subclass definition, including but not limited to creating additional subclasses, as necessary.

94. Certification of Plaintiff's claims for Class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a Class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

95. All members of the proposed Class are readily ascertainable in that Flagstar has access to addresses and other contact information for all members of the Class, which can be used to provide notice to Class Members.

96. ***Numerosity***. The Class is so numerous that joinder of all members is impracticable. The Class includes at least hundreds of thousands of individuals whose personal data was entrusted to Flagstar and compromised in the Flagstar data security breach.

97. ***Commonality***. There are numerous questions of law and fact common to Plaintiff and the Class, including the following:

- whether Defendant engaged in the wrongful conduct alleged in this Complaint;
- whether Defendant's conduct was unlawful;
- whether Defendant failed to implement and maintain reasonable systems and security procedures and practices to protect customers' and/or employees' personal data;
- whether Defendant unreasonably delayed in notifying those affected of the security breach;
- whether Defendant owed a duty to Plaintiff and members of the Class to adequately protect their personal data and to provide timely and accurate notice of the Flagstar security breach to Plaintiff and members of the Class;

- whether Defendant breached its duties to protect the personal data of Plaintiff and members of the Class by failing to provide adequate data security and failing to provide timely and adequate notice of the Flagstar security breach to Plaintiff and the Class;
- whether Defendant's conduct was negligent;
- whether Defendant wrongfully or unlawfully failed to inform Plaintiff and members of the Class that it did not ensure that computers and security practices adequate to reasonably safeguard customers' or employees' financial and personal data were used when handling Plaintiff's and the Class Members' personal data;
- whether Defendant should have notified the public, Plaintiff, and Class Members immediately upon learning of the security breach;
- whether Plaintiff and members of the Class suffered injury, including ascertainable losses, as a result of Defendant's conduct (or failure to act);
- whether Defendant breached its duties to Plaintiff and the Class as a bailee of PII entrusted to it and for which Defendant owed a duty to safeguard and of safekeeping;
- whether Plaintiff and members of the Class are entitled to recover damages; and
- whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief; and
- whether Defendant breached its duties to the Subclass under the New Jersey Consumer Fraud Act.

98. ***Typicality***. Plaintiff's claims are typical of the claims of the Class in that Plaintiff, like all Class Members, had his personal data compromised, breached and stolen in the Flagstar security breach. Plaintiff and all Class Members were injured through Defendant's uniform misconduct described in this Complaint and assert the same claims for relief.

99. ***Adequacy***. Plaintiff and counsel will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel who are experienced in Class action and complex litigation. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of other members of the Class.

100. ***Predominance***. The questions of law and fact common to Class Members predominate over any questions which may affect only individual members.

101. ***Superiority***. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a Class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of Class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class Members have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a Class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

102. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

103. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class Member.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On behalf of the Class)

104. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

105. Flagstar owed a duty to Plaintiff and Class Members to safeguard their PII. As part of this duty, Flagstar was required to retain competent third-party data transfer companies to prevent foreseeable harm to Plaintiff and the Class Members, and therefore had a duty to take reasonable steps to safeguard PII from unauthorized release or theft.

106. In other words, Flagstar was required to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

107. Flagstar's duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiff's and Class Members' PII in its possession was adequately secured and protected.

108. Flagstar further owed a duty to Plaintiff and Class Members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts.

109. There is a very close connection between Flagstar's failure to follow reasonable security standards to protect the personal data in its possession and the injury to Plaintiff and the Class. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves

from identity theft.

110. If Flagstar had taken reasonable security measures, data thieves would not have been able to take the personal information of Plaintiff and the Class Members. The policy of preventing future harm weighs in favor of finding a special relationship between Flagstar and Plaintiff and the Class. If companies are not held accountable for failing to take reasonable security measures to protect personal data in their possession, they will not take the steps that are necessary to protect against future security breaches.

111. Flagstar breached its duties by the conduct alleged in the Complaint by, including without limitation, failing to protect the PII in its possession; failing to maintain adequate computer systems and data security practices to safeguard the PII in its possession; failing to utilize adequate, updated, and secure software and related systems to protect the PII in its possession; failing to disclose the material fact that its and its vendor's computer systems and data security practices were inadequate to safeguard the PII from theft; and failing to disclose in a timely and accurate manner to Plaintiff and members of the Class the material fact of the data breach.

112. As a direct and proximate result of Flagstar's failure to exercise reasonable care and use commercially reasonable security measures, the personal data of Flagstar's employees and customers was accessed by ill-intentioned criminals who could and will use the information to commit identity or financial fraud. Plaintiff and the Class face the imminent, certainly impending and substantially heightened risk of identity theft, fraud and further misuse of their personal data.

113. As a proximate result of this conduct, Plaintiff and the other Class Members suffered damage after the unauthorized data release and will continue to suffer damages in an amount to be proven at trial. Furthermore, Plaintiff and the Class have suffered emotional distress as a result of the breach and have lost time and/or money as a result of past and continued efforts

to protect their PII and prevent the unauthorized use of their PII.

COUNT II
BAILMENT
(On behalf of the Class)

114. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

115. Plaintiff and the Class delivered their personal and financial information to Flagstar for the exclusive purpose of obtaining services.

116. The PII is intangible personal property belonging to Plaintiff and the Class Members.

117. In delivering their personal data to Flagstar, Plaintiff and Class Members intended and understood that Flagstar would adequately safeguard their personal data.

118. Flagstar accepted possession of Plaintiff's and Class Members' personal data for the purpose of providing services to Plaintiff and Class Members.

119. A bailment (or deposit) was established for the mutual benefit of the parties.

120. During the bailment (or deposit), Flagstar owed a duty to Plaintiff and Class Members to exercise reasonable care, diligence, and prudence in protecting their personal data as well as a duty to safeguard personal information properly and maintain reasonable security procedures and practices to protect such information.

121. Flagstar breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class Members' personal and financial information, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and Class Members' PII.

122. As a proximate result of this conduct, Plaintiff and the other Class Members

suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of the Class)

123. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

124. Plaintiff and the Class delivered their PII to Flagstar as part of the process of obtaining services provided by Flagstar.

125. Plaintiff and members of the Class entered into implied contracts with Flagstar under which Flagstar agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their data had been breached and compromised.

126. In providing such data, Plaintiff and the other members of the Class entered into an implied contract with Flagstar whereby Flagstar became obligated to reasonably safeguard Plaintiff's and the other Class Members' sensitive, non-public information.

127. In delivering their personal data to Flagstar, Plaintiff and Class Members intended and understood that Flagstar would adequately safeguard their personal data.

128. Plaintiff and the Class Members would not have entrusted their PII to Flagstar in the absence of such an implied contract.

129. Flagstar accepted possession of Plaintiff's and Class Members' PII for the purpose of providing services or employment to Plaintiff and Class Members.

130. Flagstar recognized that its employees' and customers' personal data is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and members of the Class. For example, the notice letter Flagstar provided to

Plaintiff and members of the Class states "Flagstar Bank treats the security and privacy of your personal information with the utmost importance…." *See* Exh. A.

131. Plaintiff and members of the Class fully performed their obligations under the implied contracts with Flagstar.

132. Flagstar breached the implied contract with Plaintiff and the other members of the Class by failing to take reasonable measures to safeguard their data.

133. As a proximate result of Defendant's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(On behalf of the Class)

134. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

135. Plaintiff and Class Members conferred a monetary benefit on Flagstar in the form of monies or fees paid for services from Flagstar. Flagstar had knowledge of this benefit when it accepted the money from Plaintiff and the Class Members.

136. The monies or fees paid by the Plaintiff and Class Members were supposed to be used by Flagstar, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and Class Members.

137. Flagstar failed to provide reasonable security, safeguards, and protections to the personal data of Plaintiff and Class Members and as a result Plaintiff and the Class overpaid Flagstar as part of the services they purchased.

138. Flagstar failed to disclose to Plaintiff and members of the Class that its practices and software and systems were inadequate to safeguard Plaintiff's and the Class Members PII

against theft.

139. Under principles of equity and good conscience, Flagstar should not be permitted to retain the money belonging to Plaintiff and Class Members because Flagstar failed to provide adequate safeguards and security measures to protect Plaintiff's and Class Members' personal and financial information that they paid for but did not receive.

140. Flagstar wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

141. Flagstar's enrichment at the expense of Plaintiff and Class Members is and was unjust.

142. As a result of Flagstar's wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Flagstar, plus attorneys' fees, costs, and interest thereon.

COUNT V
VIOLATIONS OF MISSOURI MERCHANDISE PRACTICES ACT
Mo. Rev. Stat. §§ 407.010, *et seq*.
(On behalf of the Missouri Subclass)

143. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

144. Defendant is a "person" as defined by Mo. Rev. Stat. § 407.010(5).

145. Defendant advertised, offered, or sold goods or services in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat. §407.010(4), (6) and (7).

146. Plaintiff and Missouri Subclass members purchased or leased goods or services primarily for personal, family, or household purposes.

147. Defendant engaged in unlawful, unfair, and deceptive acts and practices, in

connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Missouri Subclassmembers' Personal Information, which was a direct and proximate cause of the data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of this data breach

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Missouri Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Defendant's data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Missouri Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Missouri Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Missouri Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with

common law and statutory duties pertaining to the security and privacy of Plaintiff's and Missouri Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

148. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Personal Information.

149. Defendant intended to mislead Plaintiff and Missouri Subclass members and induce them to rely on its misrepresentations and omissions.

150. Defendant acted intentionally, knowingly, and maliciously to violate Missouri's Merchandise Practices Act, and recklessly disregarded Plaintiff and Missouri Subclass members' rights. Past data breaches put Defendant on notice that its security and privacy protections were inadequate.

151. As a direct and proximate result of Defendant's unlawful, unfair, and deceptive acts and practices, Plaintiff and Missouri Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

152. Plaintiff and Missouri Subclass members seek all monetary and nonmonetary relief allowed by law, including actual damages, punitive damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

RELIEF REQUESTED

Plaintiff, individually and on behalf of the proposed Classes, requests that the Court:

A. Certify this case as a class action on behalf of the Class and Subclass defined above, appoint Plaintiff as class representative, and appoint the undersigned counsel as class counsel;

B. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and other Class Members;

C. Award restitution and damages to Plaintiff and Class Members in an amount to be determined at trial;

D. Award Plaintiff and Class Members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;

E. Award Plaintiff and Class Members pre- and post-judgment interest, to the extent allowable; and

F. Award such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of any and all issues in this action so triable of right.

Respectfully submitted,

_____

Adam G. Taub (P48703)
ADAM G. TAUB & ASSOCIATES CONSUMER LAW GROUP PLC
17200 West 10 Mile Road, Suite 200
Southfield, MI 48075
Tel.: (248) 746-3790
adamgtaub@clgplc.net

Gary E. Mason*
Danielle L. Perry*
Lisa A. White*
MASON LLP
5101 Wisconsin Avenue NW, Ste. 305
Washington, DC 20016
Tel: 202-640-1168
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com

Counsel for Plaintiff, the Class, and Subclass